UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,428	04/05/2006	Olivier Brique	90500-000035/US	2506

30593 7590 01/06/2010

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
01/06/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,428	BRIQUE ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) _____ is/are rejected.

7)☒ Claim(s) *17-35* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. This action is in response to amendment filed 9/28/2009. Claim 17 is amended. Claims 17-35 are pending.

.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 17-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy et al. (EP 0 537971 BA and Hardy hereinafter (cited from IDS)) in view of Kupka et. al. (WO 00/30319 and Kupka hereinafter (cited from IDS)) and further in view of Takahashi et al. (US Patent Publication No. 6,507,907 and Takahashi hereinafter).

3. As to claim 17, Hardy teaches a data exchange method between two devices locally connected to one another, the first device comprising at least one first encrypting key of a pair of asymmetric keys and the second device comprising at least the second encrypting key of said pair of asymmetric keys (i.e., ...teaches a each secure terminal contain a pair of key management database [col. 4, lines 50-55] ... further teaches one for encrypting and another for decrypting [col. 4, lines 50-55]), these keys being previously initialized in the first and second device (i.e., ...teaches terminal device maintains the a key database), this method comprising: - generating, at least one first random number in the first device (i.e., ... teaches generating a random number [col., 6, lines 40-50]),

- generating, at least one second random number in the second device (i.e., ... teaches generating a random number [col., 6, lines 40-50] ...further teaches a random number is generated in each terminal [col. 7, lines 1-5]), - encrypting said first random number by said first encrypting key (i.e., ...teaches encrypting random number [col. 6, lines 40-50]), - encrypting said second random number by said second encrypting key (i.e., ...teaches encrypting random number [col. 6, lines 40-50]), - transmitting said first encrypted

random number to the second device (i.e., ... teaches random component message exchange [col. 6, lines 45-55]), - transmitting said second encrypted random number to the first device [col. 6, lines 45-55], - decrypting the first encrypted random number in said second device (i.e., ...teaches the message is process using a public key to decrypt the message [col. 6, lines 55-58]), - decrypting the second encrypted random number in said first device [col. 7, lines 10-15], - combining said random numbers generated by one of the devices and received by the other device to generate a session key (e.g., traffic key) (i.e., ... teaches combining the random to produce a third random used as a traffic key [col. 7, lines 15- 25]), - and using the session key (i.e., traffic key) to encrypt and decrypt all or part of the exchanged data between the first and second device (i.e., .. teaches using the traffic key as part of a key generation process for cryptographic process between terminals [col., 7, lines 20-35]).

Hardy does not expressly teach: - the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Hardy as introduced by Kupka. Kupka discloses: - the first encrypting key initialized in the first device during an initialization phase of the first device in a first protected environment (to provide key generation during a initialization (e.g., key built) process within a protected environment (e.g., RAM) [pg. 18, lines 5-25]).

Therefore, given the teachings of Kupka, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Hardy by employing the well known features of performing key initialization in RAM disclosed above by Kupka, for which secure data exchange between devices will be enhanced [pg. 18, lines 5-25].

The combination of Hardy and Kupka does not expressly teach:

the second encrypting key initialized in the second device during an initialization phase of the second device in a second protected environment, and

a first device of the two devices being a security module and a second device of the two being a receiver.

However, these features are well known in the art and would have been an obvious modification of the system disclosed by the combination of Hardy and Kupka as introduced by Takahashi. Takahashi discloses:

- the second encrypting key initialized in the second device during an initialization phase of the second device in a second protected environment (to provide a multi-device (e.g., protected environment) data exchange environment for which a session key (e.g., encrypting key) generation (e.g., initialization) process occur at the time (e.g., initialization) of data exchange [fig. 5]), and

a first device of the two devices being a security module and a second device of the two being a receiver (to provide two device communication environment [fig. 1A].

Therefore, given the teachings of Takahashi, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying the combination of Hardy and Kupka by employing the well known feature of key generation in a multi-device data exchange environment as shown above by Takahashi, for which secure data exchange between devices will be enhanced [fig. 5].

4. As to claim 18, Hardy teaches a data exchange method the random number (i.e., seed), generated by the first device and decrypted by the second device - is encrypted by said second device by means of said second encrypting key, - is transmitted in a encrypted form to said first device, - is decrypted in the first device by means of the first encrypting key and - is compared to said random number generated by the first device, and wherein the data transfer is stopped if the compared random numbers are not identical (i.e., ...teaches a comparison made between received decrypted encrypted seed and check data pattern with stored version .... further teaches communication synchronization is dependent on a match [col. 7, lines 50-58 - col. 8, lines 1-5]).

5. As to claim 19, Hardy teaches a data exchange method where the random number (i.e., seed), generated by the second device and decrypted by the first device - is encrypted by said first device by means of said first encrypting key, - is transmitted in

a encrypted form to said second device, - is decrypted in the second device by means of the second encrypting key and - is compared to said random number generated by the second device, and wherein the data transfer is stopped if the compared random numbers are not identical (i.e., ...teaches a comparison made between received decrypted encrypted seed and check data pattern with stored version .... further teaches communication synchronization is dependent on a match [col. 7, lines 50-58 - col. 8, lines 1-5]).

6. As to claim 20, Hardy teaches a data exchange method in which said first device and said second device contain a symmetric encrypting key, wherein the random numbers are combined with said symmetric key to generate a session key (i.e., ... teaches combining the random to produce a third random used as a traffic key [col. 7, lines 15-25] ... further teaches using the traffic key as part of a key generation process for cryptographic process between terminals [col., 7, lines 20-35]).

7. As to claim 21, Hardy teaches a data exchange method where the combination of said random numbers is a concatenation [col. 9, lines 45-55].

8. As to claim 22, Hardy teaches a data exchange method where the combination of said random numbers is a concatenation [col. 9, lines 45-55].

9. As to claim 23, Hardy teaches a data exchange method where the session key (i.e., traffic key) is regenerated in function of a determined parameter of use (i.e., ... teaches the traffic key is use as a parameter to a key generation process for cryptographic purposes [col. 7, lines 20-35]).

10. As to claim 24, Hardy teaches a data exchange method where the determined parameter of use is the duration of use [col. 7, lines 20-35]).

11. As to claim 25, Hardy teaches a data exchange method where at least one of the two devices measures at least one representative physical parameter of the communication (i.e., teaches a communication link between first and second terminal [col. 3, lines 15-20]), such as the line impedance and/or the electric consumption, where at least one of the two devices one compares the values measured to the reference values, and where at least one of the two devices acts on the data exchange when the measured parameters differ from the reference values more than a threshold value (pre\- determined number) [col. 9, lines 25-35]).

12. As to claim 26, Hardy teaches a data exchange method where at least one of the two devices acts by stopping the data exchange between the two devices [col. 9, lines 25-35]).

13. As to claim 27, Hardy teaches a data exchange method where the session key (i.e., traffic key) is regenerated in function of a determined parameter of use and wherein the determined parameter of use is the representative physical parameter of the communication (i.e., ... teaches generating a traffic key by combining two random number such that the random number [col. 9, lines 35- 58]).

14. As to claim 28, Hardy teaches a data exchange method where - at least one of the devices generates at least one supplementary random number (i.e., ... teach a random number is generated in each terminal [col. 7, lines 1-5], - this supplementary random number is encrypted by said first encrypting key [col. 7, lines 1-5], - this supplementary encrypted random number is transmitted to the second device [col. 7, lines 1-5], - this transmitted encrypted supplementary random number is decrypted in this second device [col. 7, lines 10-15], - the decrypted supplementary random number is encrypted by said second encrypting key (i.e., ... teaches a seed and pattern data is encrypted [col. 10, lines 1-5], - the supplementary encrypted random number is transmitted to the first device (i.e., ...teaches transmission of data [col. 10, lines 5-10], - the supplementary random number decrypted in the first device is compared to the initial supplementary random number generated in said first device (i.e., ... teaches decrypting and comparing data [col. 10, lines 5-15]), -the information exchange is interrupted if the comparison indicates that the two compared numbers are not identical (i.e., ...teaches terminating communication if failure [col. 9, lines 30-36]).

15. As to claim 29, Hardy teaches a data exchange method where - at least one of the devices determines at least one predefined fixed number memorized (i.e., third random number generated from combining to two random number) in the two devices [col. 9, lines 50-58], - this predefined fixed number is encrypted by said first encrypting key, - this predefined fixed encrypted number is transmitted to the second device [col. 10, lines 1-5], - this transmitted encrypted predefined fixed number is decrypted in this second device [col. 10, lines 5-10], - the predefined fixed number decrypted in the second device is compared to the predefined fixed number memorized in this second device [col. 10, lines 11- 16], - the data exchange is interrupted if the comparison indicates that the two compared numbers are not identical [col. 9, lines 30-36].

16. As to claim 30, Hardy teaches a data exchange method according where each of the numbers is encrypted separately [col. 9, lines 38-41].

17. As to claim 31, Hardy teaches a data exchange method where each of the numbers is encrypted separately [col. 9, lines 38-41].

18. As to claim 32, Hardy teaches a data exchange method where a combination of each of the numbers is encrypted [col. 9, lines 40-50].

19. As to claim 33, Hardy teaches a data exchange method where a combination of each of the numbers is encrypted [col. 9, lines 40-50].

20. As to claim 34, Hardy teaches a receiver for carrying out the method, this receiver comprising at least one calculation unit, a read-only memory, a demultiplexer, a descrambler, a digital/analog converter, an external memory and a sound and image descrambler, wherein at least the calculation unit, the read-only memory and the descrambler are contained in a same electronic chip and wherein at least one of the encrypting keys is stored in said electronic chip (i.e., ...teaches a microcontroller technology [fig. 6] ... further teaches telephone network communication [fig. 1]).

21. As to claim 35, Hardy teaches a receiver where at least one of the numbers (i.e., first number) is stored in said electronic chip (e.g., terminal) (i.e., ... teaches first random number stored in original terminal [col. 7, lines 10-15]).

Response to Arguments

With regard to applicant's remarks alleging deficiency on the part of the cited prior art in view of the claim limitation of " and using the session key to encrypt and decrypt all or part of the exchanged data between the first and second device", the Examiner contends that prior art reference Hardy discloses using asymmetric encryption for transferring data between a server (e.g., terminal A) to a client device (e.g. terminal B). Further, the Examiner contends Hardy recites that a key used to protect the transmitted data (i.e., session key) is shared between the server and client

and is used for both encryption and decryption of the transmitted data. Refer to Hardy's abstract.

Additionally, the Examiner respectfully submits that prior art reference Takahashi explicitly discloses using session key to encrypt and decrypt communication. Refer to Takahashi column 2, lines 40 – 50. The communication referred to by Takahashi is between two communicating device. Also, the Examiner respectfully submits that Takahashi discloses communication between two devices in figure 1a.

With regard to applicant's remarks alleging deficiency on the part of Takahashi pertaining to a "protective environment", the Examiner contends the basis of Takahashi's teachings are to foster an environment that protects the exchange of information between communicating devices. Refer to Takahashi's specification in substance.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431